KING&WOOD MALLESONS
金杜律师事务所

2019-20 Annual Privacy Law Update

1 Welcome to the 2019-20 Privacy Law Update

If asked to identify the defining feature of 2020, it is unlikely that 'privacy law' would quite make it to the top of anyone's list. Nevertheless, in spite of the shadow of the ongoing global disruption caused by the COVID-19 pandemic, the past 12 months have seen some significant developments in privacy and data protection law in Australia and overseas.

Indeed the pandemic has itself focussed attention on a range of privacy-related issues, from the privacy implications of contact tracing tools like the Australian Government's COVIDSafe app, to the greater cybersecurity risks we all face now that we're conducting much more of our daily lives online.

In addition, the various regulatory and government responses to the landmark Australian Competition and Consumer Commission's (**ACCC's**) Digital Platforms Inquiry report continue to attract attention. Developments in legislation, regulations and industry codes as a result of various recommendations in that report have the potential to shape the direction of privacy law in the coming months and years, including how it relates to consumer protections and media regulation.

While the consultation on broader privacy reforms that the Government promised in response to the ACCC's report has not yet commenced (at least at the time of writing), it is likely that some significant amendments – including to rules on transparency, consumer consents, and enforcement rights – will flow through in the not distant future. We expect that the more aggressive approach taken by the ACCC, the Australian Information Commissioner and the Australian Communications and Media Authority (**ACMA**) in dealing with matters relating to personal data in recent times – including the Commissioner recently launching the first ever civil penalty proceedings under the Privacy Act and the ACMA dishing out large fines for Spam Act breaches – will also continue.

Meanwhile, the first stage of the Consumer Data Right (**CDR**) has now commenced in relation to the banking industry, with the next stage set to roll out in November 2020. With other industries to then follow, the CDR has the potential to re-shape industry and consumer relationships across a number of sectors and fuel further data-based innovation and competition for the benefit of consumers for years to come. Also in the data innovation pipeline is the proposed Data Availability and Transparency Act, which is expected to reform how the Australian Government manages and shares data in the public sector in the coming year.

Further afield, the California Consumer Privacy Act is now in effect and being enforced. This development from the heart of Silicon Valley is the most significant change in United States privacy law in many years. Given the number of global technology companies to which this law applies directly, and the number of users they have around the world, including in Australia, it will likely have significant implications beyond the state of California. Elsewhere, more countries around the world introduced or progressed their own privacy law reforms and introduced mandatory notifiable data breach schemes (including over the pond in New Zealand, where a new scheme will take effect later in the year).

Privacy has also continued to feature in broader political discourse regarding the influence of large technology companies and potential threats to national security from state actors seeking to target personal data for malicious purposes. These issues will not go away, and will be some of the most important for our society to address in the coming years. In this publication, we look at a few of the key developments in Australian privacy law over the last 12 months, and look forward to some of the further changes we may expect over the next year and beyond.

2 Privacy impacts of COVID-19

The scale and impact of the COVID-19 pandemic means that it has touched almost every aspect of life this year. Certainly the privacy implications have been significant across public and private sectors of the economy. From governments seeking to carry out contact tracing and collect the information required for an effective public health response, through to private companies grappling with what information they can obtain from workers and customers in order to keep their businesses safe from the virus.

Regulatory response

In Australia, the response has been pragmatic from privacy regulators. In late March, the Commissioners and Ombudsmen with responsibility for privacy from around the country joined together to form the National COVID-19 Privacy Team to ensure a nationally coordinated response to privacy concerns.

This group issued a joint statement recognising the "significant challenges" faced by individuals, organisations and the government and acknowledging that the "use of personal information is part of addressing this public health crisis".

The key message in those early days was that while responding to the health impacts was a priority, it did not mean that privacy issues could simply be ignored. The group encouraged organisations to continue carrying out appropriate privacy impact assessments to ensure that personal information would continue to be handled in a way that was "necessary, reasonable and proportionate" during a time of rapid change.

Since then, the national regulator, the Office of the Australian Information Commissioner (OAIC), has developed a broad set of resources to assist in addressing relevant privacy issues, which are consolidated on its COVID-19 hub. These resources include more detailed statements on:

- privacy protections and obligations in connection with the COVIDSafe contact tracing app (complementing the detailed privacy impact assessment commissioned by the Department of Health, which was also made available to the public), including privacy rights FAQs for users
- guidance for businesses collecting personal information for contact tracing purposes as restrictions eased in some jurisdictions
- advice and resources on Privacy Impact Assessments, and other considerations, as employees move to work remotely and in changed working environments
- Freedom of Information guidance, updates about regulatory coordination with other countries, and a joint international statement about the importance of transparency and access to information, as well as record-keeping "in what will be a much analysed period of history"

These are valuable resources to consult in order to help ensure that your response to pandemic-related issues is consistent and aligned with recommended best practices, and also to reassure the public that their privacy rights would not be ignored or overlooked in the rush to fight the virus.

Private sector response

In response to the pandemic, many businesses were forced to shift to a remote working model. This presented a range of challenges, not least the need to find ways of maintaining information security standards and maintaining suitable oversight of workers without breaching anti-surveillance laws.

The mass adoption of some common remote working technologies led to close scrutiny of a number of existing information security and privacy practices of key technology vendors. In particular, concerns about the safety and security of video conferencing systems, led to a joint letter from privacy agencies in six countries, including the OAIC in Australia, setting out "global expectations" and principles for privacy, to promote legal compliance and also "build the trust and confidence" of users. The letter was published online and sent directly to Microsoft, Cisco, Zoom, House Party and Google, as vendors of some of the more popular video conferencing systems. Separately, providers of remote monitoring software also saw a spike in usage, but also concerns as to the potentially privacy intrusive nature of their solutions.

Security concerns were also raised in relation to services that had been offshored. Typically those services are provided from dedicated service centres, that are specifically designed to feature appropriate levels of information security. However, in many cases those centres shut down and staff were required to stay home in order to stop the spread of the virus. Setting up remote working solutions for those workers while maintaining the right standard of information security proved to be a significant challenge, particularly with workers often living in shared environments. This in turn prompted many Australian businesses to change tack by either insourcing call centre and other support roles, using existing or new onshore resources, or encouraging customers to switch to self-serve options that did not depend on

offshore support. It remains to be seen whether this will be a long-lasting trend and whether concerns about privacy and information security compliance will result in more businesses keeping critical support functions onshore in the future.

Multinational businesses attempting to deal with the impact of COVID-19 on their global workforce faced a number of unique privacy-related challenges. In particular, reconciling a range of different and potentially conflicting privacy rules across different operating jurisdictions, in order to adopt a consistent approach to dealing with COVID-19 risks has proven to be no easy task. Some, like global mining giant BHP, have developed their own internal mobile apps and other technologies to assist with contact tracing within their global workforce, reflecting that their reach may in some areas be wider than what even governments are able to achieve.

What's next?

Sadly, it seems like we will all be living with COVID-19 for some time to come. As a consequence, organisations will need to grapple with the associated data and privacy issues on an ongoing basis. We expect that smart technological solutions will be developed in response. For example, it is not hard to imagine automated systems to monitor and enforce social distancing requirements in public places like shopping malls and on public transport, by keeping track on numbers of people entering and leaving particular spaces or even tracking movement of people within those spaces. However, there will be challenges as well. For example, how will systems that rely on facial recognition cope when a significant proportion of people will be wearing masks, either because of government orders or because of ongoing caution? Some device manufacturers may already be regretting favouring facial recognition over fingerprint scanning as a method of user authentication. Just one of the many challenges of living in a post-COVID world!

3 You can teach an old law new tricks: consumer litigation risks with privacy and data compliance

Organisations dealing with consumer data and personal information, are faced with regulatory action on multiple fronts as the jurisdiction of the ACCC and the OAIC on privacy matters continues to blur. Recent actions by the ACCC are a good reminder that organisations need to think about privacy compliance outside just the narrow confines of the Privacy Act. The Australian Consumer Law has a broad prohibition against any conduct that is misleading or deceptive, or likely to mislead or deceive. There are also certain representations about goods and services that are prohibited. For financial institutions, mirror provisions exist under corporations and securities legislation and are separately enforced by the Australian Securities and Investments Commission (**ASIC**). In August 2020, ASIC commenced proceedings in the Federal Court against IOOF, arguing for breaches of financial services licensing (rather than a contravention of the Privacy Act) for allegedly failing to secure "sensitive client information including identification documents". Organisations may still fall afoul of these prohibitions, even if their data handling practices are strictly compliant with the APPs, or if they are not technically subject to the jurisdiction of the Privacy Act.

A shift in the ACCC's enforcement priorities has clearly occurred recently, and the ACCC is showing greater appetite for using its powers under the Australian Consumer Law in relation to privacy-related conduct issues. The ACCC's new concern about privacy and data was foreshadowed in the Digital Platforms Inquiry, where the ACCC's Final Report found that transparency on data management practice is critical for consumers to be able to make informed choices. While the ACCC has historically not taken consumer protection action in the privacy space, three proceedings filed in the Federal Court of Australia in recent times, including two against Google, are reflective of a change in approach.

Recent case developments

The ACCC commenced its first set of proceedings against Google in October 2019, alleging that Google did not adhere to certain representations made to Android users about user location data. In a second set of proceedings commenced in July 2020, the ACCC alleges that Google misled Australian consumers in seeking their consent to expand the scope of collected and combined personal information, including for use in targeted advertising. While these allegations are being strongly defended, the ACCC's actions put others on notice that it is willing to take an aggressive role in this space.

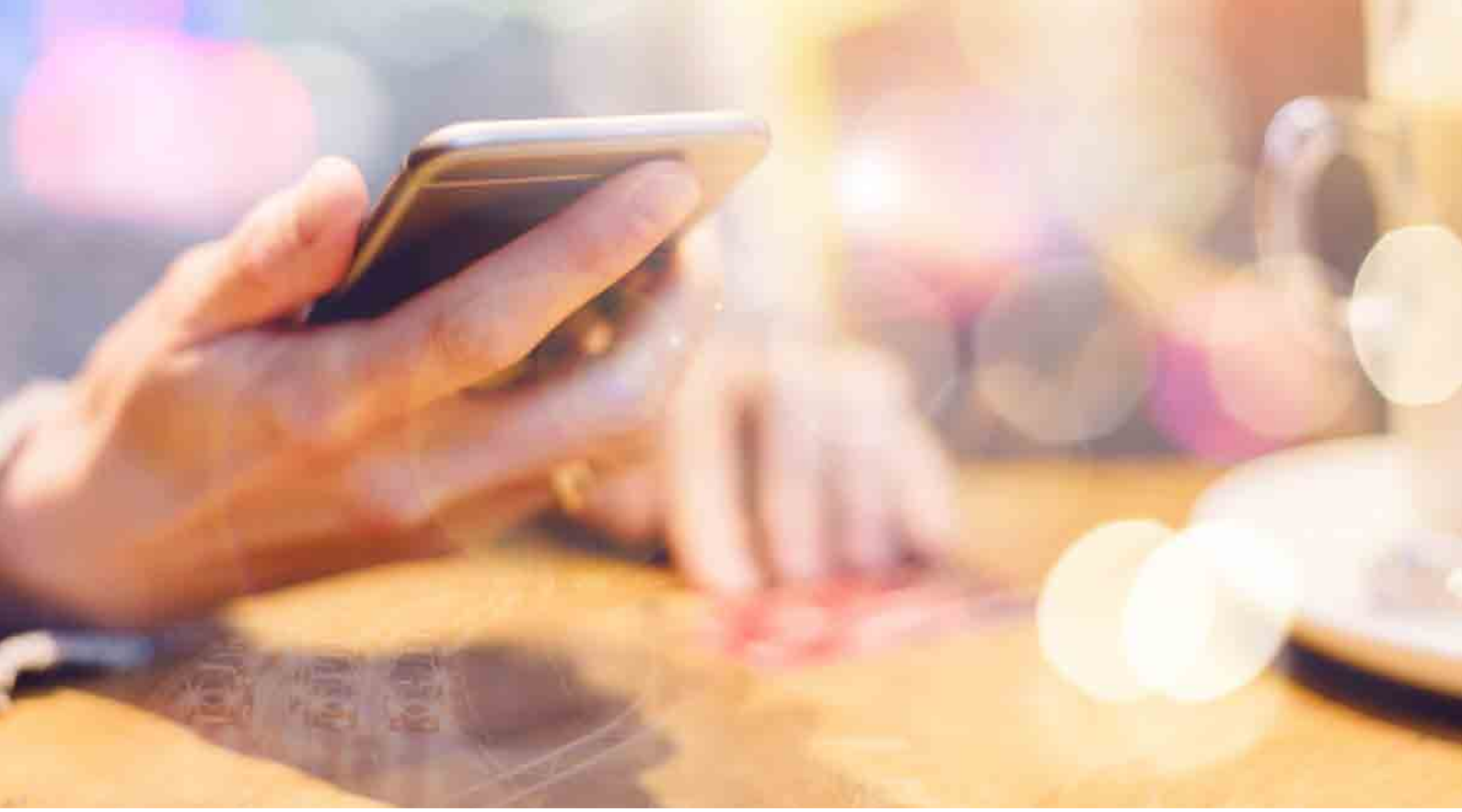
This threat was reinforced in August 2020, just before this Privacy Update went to the digital equivalent of press, when the ACCC secured a $2.9 million penalty against patient-information services provider and online booking platform HealthEngine in a privacy-related action (see ACCC v HealthEngine Pty Ltd [2020] FCA 1203). The ACCC had alleged that (amongst other practices) HealthEngine unlawfully shared patient data, including names, phone numbers, email addresses and date of birth, with insurance brokers – and in particular that individuals were not sufficiently informed that their personal information would be transferred to a third party. This was despite the fact that the relevant individuals had apparently expressly 'opted in' to being contacted to discuss their health insurance options.

The Court found this conduct was liable to mislead the public as to the nature, characteristics and/or suitability for their purpose of services provided by HealthEngine (in other words, that consumers would have expected that such contact would be a service provided by HealthEngine itself rather than a third party), and that this contravened the general prohibition against misleading or deceptive conduct in the Australian Consumer Law. The Court has also ordered HealthEngine to undertake a substantial compliance program.

New litigation, class action, and jurisdictional risk

Apart from the difficulty of dealing with the overlapping jurisdiction of two regulators concerned with privacy and data management practices, the ACCC's recent interventions presents a significant new threat for organisations that deal with consumer data for a number of reasons:

- first, while the OAIC must normally proceed by way of an investigation and determination, or by commencing civil penalty proceedings where a "serious or repeated" interference of privacy has occurred, no such procedural or threshold hurdles exist for the ACCC under the Australian Consumer Law and so the ACCC may more readily commence court proceedings on privacy-related issues;
- second, the extra-territorial operation of the Australian Consumer Law is far



broader than the Privacy Act, in that it does not require a person "carrying on business in Australia" to also be "collecting" or "holding" the relevant personal information "in Australia", which the Privacy Act does. This may give the ACCC scope to target organisations who may have been beyond the reach of the OAIC; and

- third, while private individuals cannot commence proceedings under the Privacy Act—rather they must complain to the OAIC and proceed through the OAIC's investigation process—anyone can commence proceedings for misleading or deceptive conduct under the Australian Consumer Law, including class action plaintiffs, without the same procedural hurdles. Recent experience in Australian class actions suggests that action by regulators almost inevitably leads to increased private litigation risk, particularly where litigation funding is available and damages are payable as compensation.

The broad prohibitions in the Australian Consumer Law also present new angles for would-be privacy litigants who could, for example, seek to target ancillary representations about use of encryption and other security practices, the effectiveness of de-identification techniques, and commitments made to delete or correct personal information even if there have been no underlying breaches of the Privacy Act. In addition, besides claims for misleading conduct, there are a range of other prohibitions under the Australian Consumer Law that might give rise to relevant causes of action in this area, including:

- the general ban on unconscionable conduct in trade or commerce and specific bans on unconscionable conduct in consumer and some business transactions. Conduct can be "unconscionable" if it is particularly harsh or oppressive; and
- the prohibition on unfair contract terms in consumer contracts, which could conceivable extend to privacy policies, where contracts take a position on use of consumer data that is not reasonably necessary to protect the legitimate interests of the organisation collecting and using data.

Despite the significant attention regulators are paying to this area, many organisations still adopt a "tick and forget" approach to privacy compliance. Now may well be the time for organisations to review not only privacy policies and notices, but also internal policies and procedures about handling personal information. Increasingly, regulators and plaintiffs will focus not just on narrow compliance with the Privacy Act, but also on whether data handling practices are also meeting other consumer law standards, and we expect that the ACCC's recent proceedings on these types of issues will not be the last.

4 Notes from the notifiable data breach front lines

Australian data breaches trending higher in 2020

At the end of July 2020, the OAIC released its latest report on the operation of the notifiable data breaches (**NDB**) scheme. This report covered the period between January 2020 and June 2020. The report sets out statistical information about notifications received by the OAIC under the NDB scheme, and thereby provides an overview of the nature of data breaches occurring in Australia – or at least those which are being reported under the Privacy Act.

For those late to the party, the Australian NDB scheme requires an entity covered by the Privacy Act to notify both the OAIC and any affected individuals if it has reasonable grounds to believe that an eligible data breach has occurred. This in turn depends on whether the entity has reasonable grounds to believe there has been unauthorised access to or disclosure of personal information, and whether such a breach is likely to result in serious harm to any of the affected individuals (after taking into consideration any remedial actions the entity has taken).

The NDB scheme has been in place for several years now, and the regular and detailed reporting by the OAIC has provided an interesting opportunity to identify developing compliance trends and cybersecurity risks. In that regard, while the overall number of breaches reported over the past 6 months was

lower than the prior 6 months, there were significant increases in certain areas, along with pockets of persistent compliance concerns.

Key takeaways from the most recent report

- **Number of breaches:** in the period between January 2020 and June 2020, there were 518 eligible data breaches reported to OAIC. This figure is down 3% (from 532) compared to the period between July 2019 and December 2019, but up 16% (from 447) compared to the period between January 2019 and June 2019.
- **Beware of malicious attacks:** criminal or malicious attacks were the largest cause of eligible data breaches in the most recent reporting period, accounting for 317 (61%) breaches. Although this figure represents a 7% drop compared to the period between July 2019 and December 2019, malicious attacks still pose a great threat to data security, and businesses should take this into account in planning and implementing cybersecurity defences. In particular, the OAIC reported an increase in ransomware attacks of more than 150% compared to the period between July 2019 and December 2019 (increase from 13 to 33 breaches). In light of this heightened risk, businesses should consider taking additional precautions such as network segmentation, applying additional access controls, and implementing stronger encryption to safeguard personal information against being compromised in a ransomware attack.
- **Humans continue to be a weak link:** human error caused 176 (34%) breaches reported to OAIC in the most recent reporting period. This figure is up 7% compared to the period between July 2019 and December 2019. While the overall number of eligible data breaches is down, the number of breaches due to human error is up. This is a timely reminder of the importance of effective compliance training and regular spot checks. Where possible, businesses should also consider automating systems and processes, as system faults caused only 5% of data breaches reported to OAIC in the most recent period.
- **Rise of breaches within the insurance industry:** consistent with previous periods, health, financial services and education continue to be the industries with the most data breaches. However, the report for the most recent reporting period indicated an increase in the number of data breaches within the insurance industry. Data breaches within the insurance industry accounted for 7% of all breaches notified to OAIC, making it the fourth largest source of data breaches during the period. With the amount of sensitive information that insurers collect, this is a timely reminder to those businesses to remain vigilant.
- **Significant time being taken to assess and respond:** the NDB scheme requires entities to carry out an assessment within 30 days of becoming aware of reasonable grounds to suspect that there may have been an eligible data breach, and to notify the OAIC and affected individuals as soon as practicable after it confirms that an eligible data breach has occurred. However, over the most recent reporting period there was significant variation in the time taken to conduct the assessment and notify OAIC and affected individuals. While 74% of entities completed their assessment and reported to OAIC within 30 days of becoming aware that a data breach may have occurred, 12% of all notifications took longer than 60 days, and 5% took more than 121 days. If an assessment is not completed within 30 days, the reporting entity must provide an explanation to the OAIC. The most recent report noted that in some instances "these explanations highlighted issues with regard to the entity's information handling and security practices, which in turn raised questions about broader compliance with APPs 1 and 11 regarding the security of personal information." It would be a bad outcome for an organisation if reporting a data breach sparked a wider investigation by the OAIC into their underlying privacy compliance practices. As such, organisations should have plans and processes in place to ensure that they can review and responding to potential data breaches in a timely manner.

A comparison with Canada

Canada – a country not too dissimilar to Australia in size and legal culture – introduced its mandatory data breach notification scheme in November 2018, around 9 months after the Australian NDB scheme came into effect.

Organisations regulated by the Canadian Personal Information Protection and Electronic Documents Act are required to notify both the Canadian Office of the Privacy Commissioner (**OPC**) and affected individuals, where there is a "breach of security safeguards" involving personal information that poses a real risk of significant harm to an individual. Unlike Australia, there is also a record-keeping requirement to retain records of all breaches.

In a report on risks and trends, the OPC indicated that it received 680 breach reports in the first year that mandatory reporting requirements were in effect, and that these reports indicated at least 28 million Canadians were affected by a data breach during this time. While the province of Alberta in Canada has had mandatory data breach reporting in place for many years, the OPC indicated the number of reports was much higher than expected compared with the experience in Alberta.

Some of the early trends identified in Canada closely track with the Australian experience. For example, the majority (58%) of reported breaches in Canada involved unauthorized access, with a large proportion of these breaches involving social engineering, phishing or impersonation. As in Australia, humans appear to be a significant weak link in the kinds of data breaches taking place in Canada, and malicious actors often focus their actions on one specific target. The OPC has noted that "attackers often target a small number of individuals using sophisticated psychological techniques, publicly available information, and information disclosed in other privacy breaches, to try to convince the individuals that the attacker is someone else." Accordingly, educating users in how to identify and respond safely to suspicious behaviour is critical. This is a feature of the Australian Government's recently released 2020 Cyber Security Strategy, which emphasises the role that the community – alongside government and industry – play in combatting cybersecurity risks.

As flagged above, around 34% of breaches were attributable to 'human error' in Australia in the most recent period, while in Canada around 22% of breach reports involved 'accidental disclosure'. The numbers appear to be slightly higher in Australia because the figures count 'loss of paperwork/ data storage device' as part of human

error. When combining the figures from accidental disclosure and loss in Canada, the number is also roughly 34%. If you've ever sent an email to the wrong recipient, or left your phone on public transport, it may be comforting to know that you're not alone and that people on the other side of the world are making the same mistakes! However, it does go to illustrate the importance to organisations of developing and maintaining a strict compliance culture and training their workers on how to minimise these types of slip-ups.

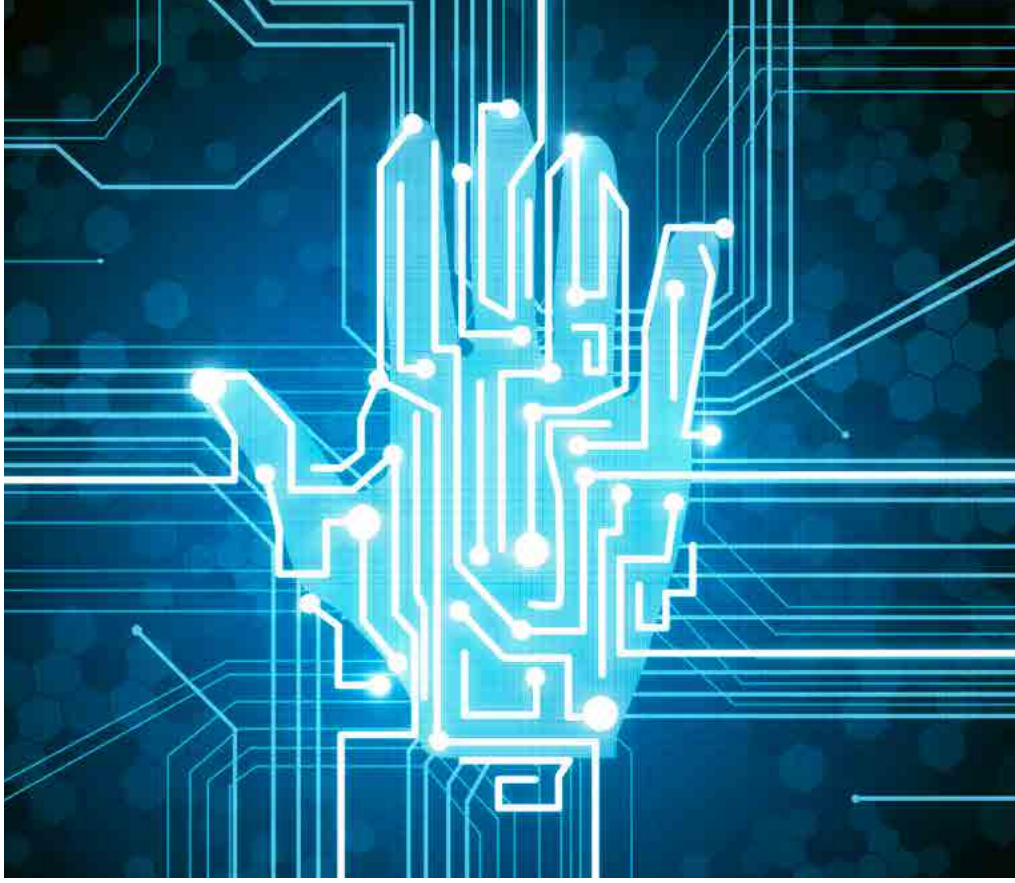
5 Privacy determinations

Each year, the Australian Information Commissioner makes a range of determinations based on privacy complaints or investigations commenced by the Commissioner on her own initiative, often including findings as to compensation and breach of the Australian Privacy Principles (**APPs**). While not final and binding, in the same way as a legal decision, these determinations are not generally challenged and may be enforced in the Federal Court. More importantly, they provide an insight into how the Commissioner interprets the APPs and views a wide range of privacy matters. Taken with a grain of salt, they are a window into the Commissioner's thinking, and even if not directly relevant to you or your organisation should serve as a useful reference point when designing an effective compliance strategy.

A trio of determinations on non-economic loss

In June of this year, the Commissioner published three determinations that together provide a useful insight into how the Commissioner will assess compensation for non-economic loss and aggravated damages.

While Australian law remains far from developed in this area, and these determinations are only a small sample of the Commissioner's thinking, they appear to be increasingly common – with many of the determinations made in 2019 and 2020 containing an award for this kind of compensation. It is an issue that organisations would do well to monitor, with the introduction of a direct right of action for individuals being one reform that the Government will likely consider in the near future, in which case we might see a significant rise in privacy litigation in the future.



a. 'ST' and Chief Executive Officer of Services Australia [2020] AICmr 30 (30 June 2020)

This determination relates to a disclosure of personal bank statement information by a child support agency to an ex-partner in the course of child support assessment proceedings in a tribunal review process. The complainant alleged that the bank statement revealed places she frequented, which had the potential to cause the individual harm if disclosed to her ex-partner. The Commissioner accepted that the complainant was in fear of the ex-partner, and a Family Violence Order had previously been obtained.

The Commissioner found that the disclosure of the information amounted to a breach, as it was neither required or authorised by law, nor was the complainant reasonably likely to have been aware or made aware that the information may be disclosed in this type of circumstance.

The Commissioner awarded $3,000 to the complainant. In assessing the measure of compensation to be awarded, the Commissioner considered the power under section 52(1AB) of the Privacy Act to award damages for humiliation or injury to the feelings of the individual, and found the privacy breach had caused the individual distress. However, the Commissioner also noted that the degree by which the disclosure contributed to the individual's fear of being located was "not significant" and that in some cases, these locations had previously been disclosed to the ex-partner.

Key takeaways:

The OAIC has the power to award damages for the complainant's non-economic loss in the form of humiliation or injury to feelings.

Establishing causation may be more difficult in cases of non-economic loss, especially where other factors may be at play and have contributed to the same harm.

b. 'SF' and 'SG' [2020] AICmr 22 (19 June 2020)

This determination relates to a psychologist who refused to give an individual access to their own clinical records or provide written reasons for the refusal.

The Commissioner found that the psychologist was in breach of APP 12.1 by failing to give access to personal information they held about an individual with no relevant exception applying. Further, by failing to notify the individual of the grounds for refusal to give access, the psychologist was also in breach of APP 12.9, which requires reasons to be given for a refusal.

The Commissioner concluded the privacy breach had been a "contributing factor" to some harm suffered by the complainant, including distress and re-traumatisation, and awarded $3,000 in compensation. When assessing compensation for non-economic loss in the form of psychological injury and distress, the Commissioner noted that it was "very hard to disentangle" the harm caused by the privacy breach from harm caused by the individual's previous dealings with the psychologist and the individual's participation in other proceedings regarding the psychologist's registration.

The Commissioner also found the psychologist's conduct to justify the awarding of aggravated damages to the amount of $2,000. The Commissioner noted the psychologist had acted in a way that was insulting to the individual and demonstrated a disregard of the individual's privacy rights. Contributing to this view was the psychologist's failure to engage with the OAIC until late in the investigation and tone when doing so – for example, one response from the psychologist was to state "I will not give credence to her accounts by responding to each one, but be assured she … is held in low repute by most people in the area." This, in the Commissioner's view, exacerbated the injury.

Key takeaways

Although it may sometimes be difficult to 'disentangle' the non-economic loss caused by the privacy breach from other causes, the OAIC may find a causal link and make an award of compensation where the breach was a "contributing factor" to some of the harm.

Aggravated damages might also be awarded where the OAIC finds that the respondent's attitude in engaging with the complaint and/or investigation, including any delays, exacerbated the complainant's injury.

c. 'SD' and 'SE' and Northside Clinic (Vic) Pty Ltd [2010] AICmr 21 (12 June 2020)

This determination relates to a disclosure of personal and health information about two individuals (including their HIV positive status) by a medical clinic by twice emailing an incorrect Gmail email address.

The Commissioner found the clinic breached APP 6, by disclosing the personal information for a secondary purpose with no relevant exception applying, and also APP 11.1, by failing to take steps to protect the information from unauthorised disclosure.

The Commissioner awarded compensation for psychological injury and distress arising out of the disclosure, as well as economic loss resulting from the first complainant's need to seek psychological treatment. As to the magnitude of compensation, the Commissioner considered the harm to be "within the mid-range for distress and hurt" (in the realm of $7,500 to $8,500), being two 'one-off' disclosures to a single private email address, as opposed to a high-range harm, where disclosure is to the "public at large over a sustained period of time".

The Commissioner noted that, although the disclosure was a result of human error and not 'malicious intent', that went only to the assessment of aggravated damages and not the base amount of compensation for the injury caused. Ultimately, the Commissioner did not consider the clinic's conduct to be of such a degree or character as to award aggravated damages.

Key takeaways:

The magnitude of compensation awarded for non-economic harm owing to unauthorised disclosure may be influenced by the size of the audience and prolongation of disclosure. A disclosure may be of a 'higher range' where it is made to the public at large over a sustained period of time.

The fact that a privacy breach was accidental will not affect the measure of compensation awarded, but may go towards the Commissioner's consideration of aggravated damages.

Risks regarding collection of public material

The determination in 'RC' and TICA Default Tenancy Control Pty Ltd (Privacy) [2019] AICmr 60 is an interesting case study in issues that arise when using public information.

TICA Default Tenancy Control Pty Ltd (**TICA**) maintained a database which collated publicly available information including daily court lists, and was available to real estate industry professionals for a fee. The complainant was party to a proceeding which was listed in the database, and her name was listed in the entry without her knowledge or consent. The proceeding was discontinued, and the database was not updated. The complainant became aware of the database entry when she made a private rental application and the real estate agent asked her if she was the person in the entry, which she confirmed. The complainant alleged she was unable to secure a private rental because of adverse inferences made by the real estate agent from the database entry. The information was collected in mid-February 2014, just before the APPs commenced, meaning the National Privacy Principles (**NPPs**) (the precursors to the APPs for private sector organisations) applied.

TICA argued the database entry was not personal information because the complainant was not identifiable from the entry, on the basis that it contained no unique identifiers such as date of birth, and that the complainant's name was not unique. However, the Commissioner applied the standard view, based on Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4, that the individual's identity did not need to be apparent solely from the information for the information to qualify as "personal information". If the individual's identity could be reasonably ascertained from other available resources, it may still be personal information. In fact, the real estate agent was able to ascertain the complainant's identity from the information in the listing combined with the rental application information. In context, the Commissioner concluded the listing contained personal information.

Importantly, the fact that the information was publicly available did not detract from the fact it was personal information, and the Commissioner determined that in their view "the downloading, or obtaining, of that information from publicly available sources is the 'collection' of the material". The Commissioner determined that even though the information was posted publicly, TICA did not take reasonable steps to ensure the individuals were aware of the matters required to be notified on collection (in breach of the transparency obligations in NPP 1.5, which have since been superseded by equivalent obligations under APP 5). The Commissioner accepted that there were no reasonable steps TICA could have taken to bring the collection to the attention of the complainant specifically, acknowledging the difficulty of obtaining the contact details of individuals, but that it could have made individuals generally aware of its collection activities on a publicly-accessible part of its website. This is a slightly surprising finding, given that there was no indication the complainant would have been likely to visit the TICA website (other than perhaps after discovering the information had already been included in the database, at which point such notice would hardly reduce the alleged harm)! This means that entities that collect and collate information from public databases still need to be mindful of their transparency obligations, and to provide notice of their collection activities to the extent they are able to do so (e.g. by including notices on their own website).

Separately, the Commissioner found that TICA did not breach its obligations with respect to use and disclosure (under NPP 2), or data quality, and maintaining accurate, complete and up-to-date records (under NPP 3 or NPP 10), because the database was a historical point-in-time, and so remained accurate even if the proceeding was discontinued. Interestingly, under the then-applicable version of the Privacy Act, section 16B(2) provided that the Act only applied to information which is 'held in a record', and that records exclude 'generally available publications'. While the determination mentions the provisions of the then-applicable section 16B(1) on 'generally available publications' in relation to collection, it seems to ignore section 16B(2) in the analysis of all of the other NPPs. There is no discussion about whether the court lists, or the TICA database, were generally available publications and the impact this might have on the application of the Act. While this may not have changed the overall outcome, since no breaches were found other than in relation to collection, it's not clear if this was an oversight or merely a missed opportunity for further clarity on this aspect of the law.

The complainant sought compensation of $7,700 for economic loss associated with finding alternative accommodation, and $5,000 for pain and suffering. The causal connection between the privacy and the economic loss was not sufficiently made out, but $1,500 was awarded for non-economic loss.

Key takeaways:

The collection obligations under the Privacy Act still apply to information collected for inclusion in a 'generally available publication', even though other obligations may not. This remains true in the latest version of the Privacy Act (although some changes have been made).

Where it is not practicable to notify an individual directly that their personal information has been collected, it may still be necessary to consider other reasonable steps which could be taken to fulfil relevant transparency obligations, such as placing a notice on a public website.

A database that provides a "point-in-time" capture does not necessarily become out of date (for example, for the purposes of APP 10) if the facts are true at the time of capture, and that is made clear on the face of the database.

6 The OAIC and the CDR Privacy Safeguards

First announced in November 2017, the Consumer Data Right (**CDR**) aims to create a new data economy in Australia by giving consumers greater control over the accessing and sharing of their data. The CDR commenced on 1 July this year with the launch of the first stage of Open Banking. Subsequent stages will expand the range of data, and the range of service providers, covered by Open Banking. The CDR will launch next in the energy sector which is expected to be followed by the telecommunications sector and eventual rollout economy-wide. Much has been written on the CDR – not least by KWM, a lot of which you can find on our website – but in this context, we want to highlight the privacy safeguards and role that the OAIC will play in the regime.

Meet the regulators:

There are three key regulators that will help to manage the legal framework for the CDR:

- the ACCC will act as the lead regulator, including by making the CDR Rules, accrediting potential data recipients, and monitoring compliance and taking enforcement action where necessary;
- the OAIC will be responsible for applying the dedicated privacy safeguards that have been designed into the CDR regime and will be the primary handler of privacy-related complaints, supported by a range of investigative and enforcement powers to carry out this function; and
- the Data Standards Body (**DSB**) will be responsible for the creation of the technical standards for the sharing of consumer data under the CDR framework. The current version of the standards is available at: Consumer Data Standards.

What are the Privacy Safeguards?

The privacy safeguards are legally binding statutory provisions that seek to protect the security and integrity of the CDR regime. They are a critical feature of the regime, given the potentially sensitive nature of CDR data. There are 13 separate safeguards that apply similar protections to those that apply to the handling of personal information under the APPs. However, in some instances, the CDR privacy safeguards expand on these protections. For example, there is no equivalent APP for CDR Privacy Safeguard 10, which requires an accredited data recipient to notify the consumer when they disclose CDR data.

The OAIC has released guidelines outlining how it intends to apply the CDR privacy safeguards and exercise its associated powers and functions. These guidelines set out not only the OAIC's view on minimum standards for compliance, but also examples of good privacy practice to supplement those standards. Given this is a wholly new area, without any established precedent or regulatory practice, these guidelines will be an important reference point for businesses when designing their own compliance processes and procedures.

Businesses should be aware that the maximum penalties for non-compliance with the privacy safeguards under the CDR regime are higher than those that currently apply under the Privacy Act. In particular, while penalties are limited to a maximum of $420,000 for individuals and $2.1 million for corporations under the Privacy Act, the maximum penalties that apply for the CDR privacy safeguards are established under the Competition and Consumer Act and for corporations will be the greater of $10 million, three times the value of the benefit obtained that is reasonably attributable to the contravention, or if the benefit is unable to be determined, 10% of annual turnover in 12 month period following the contravention. This asymmetry may be temporary, however, as the Government has previously indicated an intention to update the Privacy Act penalty provisions to align with this same standard. In any event, these higher penalties should serve as a warning to prospective participants in the CDR regime to not focus only on the potential for expanded use and sharing of data, without balancing that against the need to maintain appropriate privacy compliance standards.

7 Schrems wins round 2 as international data transfers get more complicated

The end of the Privacy Shield

Austrian privacy law campaigner Max Schrems has had a second major victory in the European Court of Justice (**CJEU**), effectively bringing an end to the "Privacy Shield" as a mechanism for the transfer of data from the European Union to the United States.

The Privacy Shield was put in place soon after the CJEU struck down its predecessor, the "Safe Harbour" regime in 2015, in a case also brought by Mr Schrems. That lasted just 5 years, and the latest decision (affectionately dubbed **Schrems II**) means that EU organisations relying on the Privacy Shield for personal data transfers to the US will no longer be lawfully able to do so.

As there are very few countries which have been officially declared as ensuring "an adequate level of protection" required by the GDPR (the list is available here, and absent the Privacy Shield the US is not on it, though nor is Australia for that matter), organisations will instead need to rely on mechanisms such as the EU's Standard Contractual Clauses ("SCCs") or Binding Corporate Rules ("BCRs"), as well as careful due diligence of service providers.

The central issue in the Schrems II case was whether use of personal data of EU citizens was subject to sufficient safeguards and recourse for those European individuals under the Privacy Shield. Schrems argued that content and metadata sent to US-based entities under the Privacy Shield scheme was subject to surveillance and security measures of US authorities, and that no recourse was available to EU citizens to object to such processing. For Schrems, this rendered the Privacy Shield severely compromised, since the "adequate" protections in reality were not offered by the US data protection regime, and the CJEU agreed.

Data nationalism is a growing force

While the end of the Privacy Shield only directly affects transfers of data from the EU to the US, the Schrems II decision is far from the only barrier being raised around the world for cross-border data flows.

Governments around the world have been actively considering potential concerns – ranging from privacy to national security – that may arise from allowing data about citizens to move offshore. Where changes are being proposed, the trend has been to require more data to remain onshore. The Schrems II decision reinforces the starting position that personal data of EU citizens in the EU is expected to stay in the EU – or at least stay subject to its legal protections. India has stepped up actions on keeping data of its 1.4 billion citizens within the country, including banning 59 apps (the most prominent of these being TikTok) with links to China. China's national cybersecurity laws contain a number of strict data sovereignty requirements for personal information and other "important data". Australia has not been exempt, with the Foreign Investment Review Board imposing data sovereignty conditions on a number of foreign investments into Australia, and foreign investment rules currently being subject to further review, which may lead to the introduction of additional restrictions on investments in businesses that control sensitive data.

For many large organisations that operate across multiple jurisdictions, the ability to manage data from centralised "data lakes" is standard practice – but increasingly stringent data sovereignty requirements and the absence of a harmonised international approach to privacy regulation may eventually drive some towards a more decentralised approach.

8 The Western Front: American developments in privacy led by the CCPA

Somewhat out of step with many parts of the world, the United States has been relatively slow to adopt extensive privacy-specific legislation at either the state or federal level – until now. The California Consumer Privacy Act (**CCPA**) came into effect on 1 January 2020, introducing a variety of new privacy protections for Californian consumers and associated compliance obligations on those who "do business" in California, the home of Silicon Valley.

While the focus of the CCPA is relatively narrow, aimed at providing protection for residents of California, it is widely expected to have national implications, not only because of the number of organisations which do business in California (the home of Silicon Valley and many world leading technology companies) but also as an indicator of the direction other US jurisdictions may take when considering the need for their own dedicated privacy laws. Some commentators view the introduction of the CCPA as a symptom of the inability for a cohesive federal privacy law to gain traction in the US – leaving the potential for a more fragmented state-based approach that may be more difficult and costly to comply with.

There are some interesting comparisons that may be drawn between the CCPA and Australian privacy law. For example the definition of 'personal information' used in the CCPA is, as is the case in Australia, broadly defined and linked to information that identifies, relates to, describes, or is reasonably capable of being associated or linked with a consumer or household – but unlike in Australia it expressly excludes information made publicly available in government records. Under the CCPA, individuals have rights to access their personal information, and to know certain information about its collection and use, similar to Australia. But the CCPA also includes rights to restrict the sale of personal information, a right to request deletion, and a right not to be discriminated against for exercising privacy rights.

The "do not sell" provisions have perhaps received the most attention, likely due to the new procedures which many businesses had to put in place to comply (including by placing a "do not sell my personal information" option on relevant websites to enable consumers to exercise their opt-out rights). Another notable feature is that businesses may offer "financial incentives" on an opt-in basis to compensate consumers for the user of their data (e.g. by offering discounts if consumers are willing to have their information shared or sold to third parties) but not if those incentives are "unjust, unreasonable, coercive, or usurious in nature". This will be a fascinating area to monitor for economists who have been working on assessing the value of data. Apart from these areas, there are many other nuances in the CCPA – including as to the scope of information that it covers, and the application and scope of the various consumer rights that it creates – that may pose significant challenges in the long term for the management of personal information in a multi-jurisdictional or global business.

All eyes on California

Enforcement of the CCPA commenced much more recently, on 1 July 2020, so the impact the CCPA will have in practice is still to be seen. But given the attention these developments have received at the headquarters of some of the world's largest technology companies, it seems safe to say it will be worth keeping an eye on how things move forward, no matter where you are in the world, as the CCPA requirements will likely play a significant role in shaping the attitudes and approaches that these companies take to privacy compliance across their global businesses.

We've got you covered
KWM National Team

Michael Swinson
Partner, Melbourne
TMET, IT & Data
T +61 3 9643 4266
M +61 488 040 000
michael.swinson@au.kwm.com

Bryony Evans
Partner, Sydney
TMET, IT & Data
T +61 2 9296 2565
M +61 428 610 023
bryony.evans@au.kwm.com

Patrick Gunning
Partner, Sydney
IP Commercialisation
T +61 2 9296 2170
M +61 418 297 018
patrick.gunning@au.kwm.com

Cheng Lim
Partner, Melbourne
TMET, IT & Data
T +61 3 9643 4193
M +61 419 357 172
cheng.lim@au.kwm.com

Cal Samson
Solicitor, Melbourne
T +61 3 9643 4166
M +61 437 652 995
Cal.Samson@au.kwm.com

Madeline Close
Solicitor, Melbourne
T +61 3 9643 4302
M +61 417 059 845
Madeline.Close@au.kwm.com

Madeline Howard
Law Graduate, Sydney
T +61 2 9296 2658
M +61 418 401 302
Madeline.Howard@au.kwm.com

Alison Thompson
Solicitor, Sydney
T +61 2 9296 2564
M +61 413 257 821
Alison.Thompson@au.kwm.com

James McGrath
Solicitor, Sydney
T +61 2 9296 2312
M +61 436 306 691
James.McGrath@au.kwm.com

Lauren Murphy
Solicitor, Melbourne
T +61 2 9296 2071
M +61 400 490 247
Lauren.Murphy@au.kwm.com

Luke Hawthorne
Senior Associate, Sydney
T +61 2 9296 2114
M +61 437 515 203
Luke.Hawthorne@au.kwm.com

Special thanks to Cal Samson for his role as editor.

www.kwm.com

Asia Pacific | Europe | North America | Middle East